RISK

ANALYSIS

Real Estate Assessment Center (REAC)
Financial Assessment Subsystem (FASS-PH)

U.S. Department of Housing and Urban Development

July 11, 2005

System:	REACS
Subsystem:	FASS-PH
Release:	8.1.0.0
Database Release:	REACS
Doc Type:	Risk Analysis Plan
Doc Date:	07/10/05
Doc Author:	Avineon/Virginia Davis
Doc Number:	1.2
Doc Status:	Final

Revision Sheet

Release No.	Date	Revision Description
1.0	04/20/05	Draft Risk Analysis Plan for Proposal of FASS-PH project
1.1	05/31/05	Draft Risk Analysis Plan for PM and GTM approval
1.2	07/11/05	Final Risk Analysis Plan for Deliverable Submission
1.3	10/27/05	Revise Risk Analysis Plan to incorporate GTM comments

Risk Analysis Authorization Memorandum

I have carefully assessed the Risk Analysis for the Financial Assessment Subsystem – Public Housing (FASS-PH). This document has been completed in accordance with the requirements of the HUD System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____	_____
Freddie Harrison FASS-PH IT Manager (HUD)	JULY 10, 2005
_____	_____
Nicholas Miele FASS-PH Business Program Manager (HUD)	JULY 10, 2005

RISK ANALYSIS

TABLE OF CONTENTS

Page #

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

1.1 Purpose

The Risk Analysis Plan is the third plan included in the Project Management Plan package. The plans included in the Project Management Plan package are:

1. **Project Plan**
2. **Transition Plan**
3. **Risk Assessment Plan**
4. **Quality Assurance Plan**

In order to establish the context for the Risk Assessment Plan, we must first define the relationship of this plan to the other plans included in the Project Management Plan package in simple terms. To do this, we will make the following assumptions. The Project Plan states the objective of the work to be done and ***what*** tasks are needed to accomplish this objective. The Transition Plan provides a baseline of the current situation and the supporting tasks needed to shift the responsibility of the tasks from the incumbent team to the current team. The Transition Plan also provides details on extenuating circumstances that may affect the overall objective of the project. The Risk Analysis Plan provides the philosophy of ***why*** the conditions relating to the tasks needed to accomplish the objective should be identified, analyzed and tracked to prevent failure. The Risk Analysis Plan also defines the framework and resulting strategy that the current team will employ to minimize probability of risk as well as reduce the impact of risks that evolve from probability to reality during the course of the software development lifecycle. The Quality Assurance Plan describes ***how*** the current team will assure task robustness (i.e., assure objective of each task by controlling the conditions of the task) as a means of guaranteeing the objective of the project.

The purpose of the Risk Analysis Plan is to describe the principal, methodology, and strategy of implementing risk management activities in the Financial Assessment Subsystem - Public Housing (FASS-PH) Release 8.1. Specifically, this plan will cover:

1. **Risk Analysis**
    - Provide a definition of risk
    - Explain how variations of conditions on a task are interpreted to be a risk
    - Describe the metrics used to predict risk, ability to detect risk, risk impact, as well as likelihood of risk
    - Provide plan for identification and collection of risk statements
2. **Risk Management**
    - Define the concept of Continuous Risk Management

- Explain the processes used to assure robustness of task (i.e., preventing risk through assuring the success of task by increasing the condition variables in which success can be realized)[1]

- Explain the process used to determine when a risk requires mitigation (i.e., reduce the negative impact on the outcome of a task when the conditions for the tasks are not "ideal").

- Provide plan for management and communication of risk status

- Describe the strategy employed to activate contingency plans

3. Risk Control

- Describe the strategy of tracking risk with the objective of controlling condition variations on a task[2]

- Describe the format and objective of traceability as it pertains to risk

- Describe the relationship between Quality Assurance efforts and Risk Management

1.2 Scope

This Risk Analysis Plan relates to the Housing and Urban Development's (HUD) Financial Assessment Subsystem – Public Housing (FASS-PH). The work to be performed pertains to software development. Therefore, this plan will address risks specific to software development tasks.

The contract for FASS-PH software development tasks has been awarded to a new team and many of the risks identified may initially relate to transition. The previous team identified risks related to tasks that are in progress or being considered for future releases. Many of these risks remain valid and will be added to those risks that the new team identifies.

1.3 System Overview

The FASS-PH is a subsystem of the Real Estate Assessment Center System (REACS). FASS-PH will help enable centralized financial analysis that can be used to identify where HUD should focus its limited resources to improve service delivery and manage its housing programs proactively. To achieve this goal, the following objectives have been identified:

- Gather standard financial data pertaining to each Public Housing Agency (PHA) and Section 8 Entity by combining standard fiscal audit information with reporting and compliance factors as defined by the Single Audit Act;
- Assess the financial condition of all PHAs and Section 8 Entities using a comprehensive protocol;
- Assess financial risk using standard financial data;

[1] The assurance task robustness is covered in detail in the Quality Assurance Plan.

[2] Again, many of the topics covered in the Risk Assessment Plan will be reiterated in other plans included in the Project Management Plan due to the relationship of the plans to each other.

- Determine an objective, numerical score for each PHA and Section 8 Entity using standard protocols for financial performance review;
- Enable HUD staff to focus on the most troubled PHAs and Section 8 Entities based on the risk associated with the score;
- Eliminate or address existing material weaknesses identified through IG Audits. This includes mitigating potential risks;
- Support HUD's mission;
- Implement OMB Circular A-123 compliant policies and procedures;
- Support HUD's eGov Strategic Plan;
- Automate paper based forms to support the Government Paperwork Elimination Act (GPEA);
- Provide payback as early in the system lifecycle as possible;
- Provide significant benefits to HUD;
- All new functionality meets the Rehabilitation Act Section 508 requirements.

System General Environment

The following table identifies the general environment for the development of FASS-PH:

System Environment Table	
Environment	**System / Organization**
System	Real Estate Assessment Center System (REACS)
Subsystem	Financial Assessment Subsystem - Public Housing (FASS-PH)
Responsible Party Description	
Sponsor	Public and Indian Housing – Real Estate Assessment Center (PIH-REAC)
Requirements	Avineon Inc.
Design	Avineon Inc.
Development	Avineon Inc.
System and Integration Testing	Avineon Inc., DCG
User Acceptance Testing	To be determined byPIH -REAC Management
Deployment	Avineon Inc., DCG
Maintenance	Avineon Inc., DCG
System Environment, Code, and Category: and Operational Status Description	
PCAS	307820
System Code	P093
System Category	Non-Major
Operational Status	Operational
System Environment	Web Based

1.4 Project References

Provide a list of the references that were used in preparation of this document.

- HUD SDM Risk Analysis Plan Template
- Incumbent's Documentation regarding current FASS-PH Risk Assessment
- Task Order Request and Response: GSC-TFMG-05-31210 and accompanying Risk plan
- Capability Maturity Model Integrated (CMMI)[SM] Systems Engineering, Software Engineering, Integrated Process and Product Development
- FASS-PH Business Requirements Documents (BRD) provided by HUD to the current team

1.5 Acronyms and Abbreviations

Table 1-2 is a list of acronyms and abbreviations used in the Risk Assessment Plan. A full list of acronyms and abbreviations used in the Project Management Plan is provided in the Project Plan.

Acronym	Detail
BRD	Business Requirement Document
CCB	Change Control Board
CM	Configuration Management
CMMI	Capability Maturity Model Integrated
CRM	Continuous Risk Management
CTC	Condition-Transition-Consequence
DBA	Database Analyst
DCG	Development Coordination Group
GTM	Government Technical Manager
HUD	Department of Housing and Urban Development
HUDWeb	HUD's internet
ID	Identification
Int.	Intermediate
IT	Information Technology
LAN	Local Area Network
LOE	Level of Effort
MF	Multi-Family
MSP	Mitigation Strategy Planning
Ops	Operations
PDA	Personal Digital Assistant
PIH	Public and Indian Housing
PM	Project Manager
POC	Point of Organizational Contact
QA	Quality Assurance
RAP	Risk Analysis Plan
REAC	Real Estate Assessment Center

RI&A	Risk Identification and Analysis
SDM	Software Development Methodology
SEI	Software Engineering Institute
SME	Subject Matter Expert
SQL	Structured Query Language
Sr.	Senior
SRE	Software Risk Evaluation
TBQ	Taxonomy Based Questionnaire
UML	Unified Modeling Language
WASS	REAC Security Subsystem
WBS	Work Breakdown Structure

Table 1-1

1.6 Points of Contact

1.6.1 Information

Table 1-3 is a list of the points of organizational contact (POC) that may be needed for informational and troubleshooting purposes.

Contact Type	Contact Name	Department	Telephone Number	E-mail Address
HUD FASS-PH IT Manager	Freddie Harrison	IT Manager	202-475-8639	Freddie_Harrison@hud.gov
HUD FASS-PH Business Manager	Nicholas Miele	Director – PHAS Operations	202-475-8788	Nicholas X. Miele@hud.gov
Project Manager	Keith Bennett	Avineon, Inc.	202-475-8903	Keith_Bennett@hud.gov
QA Manager	Virginia Davis	Avineon, Inc.	202-475-8888	Virginia_N._Davis@hud.gov
Account Manager	Hee Sun Choung	Avineon, Inc.	703-671-1900 x. 208	HChoung@Avineon.com
HUD REAC IT Lead	John Zuber	HUD Real Estate Assessment Center	202-475-8832	John_Zuber@hud.gov

Table 1-2

1.6.2 Coordination

Table 1-4 is a list of organizations that require coordination between the project and its specific support function as well as a proposed schedule (coordination interval) for coordination activities.

Organization	Support Function	Coordination Interval

PIH REAC FASS-PH	Business requirements support, project management	Continuous, Weekly meetings at minimum
PIH REAC FASS-PH IT	Business/functional/system requirements, design, development, testing, maintenance	Continuous
PIH REAC Development Coordination Group (DCG)	Development coordination, installation, deployment.	Continuous, Weekly (Change Control Board [CCB] Meetings) at minimum
HUD IT	Implementation coordination, installation, deployment	Continuous, As Needed
RELATED SUBSYSTEMS	Interface requirements support, development coordination	Weekly (Change Control Board [CCB] Meetings) at minimum, As Needed

Table 1-3

2.0 PROJECT AND SYSTEM DESCRIPTION

2.0 PROJECT AND SYSTEM DESCRIPTION

2.1 Summary

FASS-PH is a mission critical system for HUD. Specifically, FASS-PH is a subsystem of the Real Estate Assessment Center system (REACS).[3] The application provides trend, performance and compliance analyses, PHA profiles, standardized monitoring checklists, results of document reviews, summaries of review results suitable for inclusion in monitoring reports, and summaries of review activities. The system also is utilized for tracking review timeframes or providing that information to a centralized event tracking system.

Additionally, FASS-PH provides a knowledge base that is utilized for current compliance requirements, self-assessment tools for PHAs and referrals to PHAs with exemplary practices. The System Knowledgebase Administrator is responsible for maintaining the legislation, policy, procedures, and rules changes.

The FASS-PH subsystem interfaces with several other PHAS subsystems within the REAC environment. This integration allows the FASS-PH subsystem to provide information more readily to the user from different interface points, easing the user experience. This permits data entry to be more fluid.

System Environment	
System	Real Estate Assessment Center System (REACS)
Subsystem	Financial Assessment Subsystem - Public Housing (FASS-PH)
Sponsor	Public and Indian Housing – Real Estate Assessment Center (PIH-REAC)
PCAS	307820
System Code	P093
System Category	Non-Major
Operational Status	Operational
System Environment	Web Based
Requirements	Avineon Inc.
Design	Avineon Inc.
Development	Avineon Inc.
System and Integration Testing	Avineon Inc., DCG
User Acceptance Testing	To be determined by PIH-REAC Management
Deployment	Avineon Inc., DCG
Maintenance	Avineon Inc., DCG

[3] Section C.1.2.1 of HUD Task Order Request (TOR) GSC-TFMG-05-31210 for Financial Assessment Subsystem-Public Housing (FASS-PH)

2.1.1 Project Management Structure

Table 2-1 provides the basic aspects of the project management structure of the FASS-PH Release 8.1.0.0.

Aspect	Detail
Project Sponsor	PIH-REAC
Sponsoring Office Project Leader	Freddie Harrison (FASS-PH IT Manager)
Project Start Date	April 25, 2005
Project End Date	October 26, 2005

Table 2-1

2.1.2 Project Staffing

Table 2-2 provides the number of contractor staff hours required as well as identifies the expertise level (Senior shown as Sr. and Intermediate shown as Int. in Position column) and skill set (Skill Category column). The skill category is further defined by whether the skill category is considered technical or program related. The contractor staff hours are broken down by each skill category. This information will help management determine the resources required and when they are needed.

Position	Skill Category	Technical/Program Related	Staff Hours (per week)
Project Manager	Project Management, CMMI	Program	40 hours
Systems Analyst/ Sr. Programmer	Requirements, UML, ColdFusion, SQL, Testing	Technical	40 hours
Sr. Software Developer (2)	UML, Java, ColdFusion, SQL	Technical	40 hours
Sr. Systems Test Engineer	UML, Java, ColdFusion, SQL	Technical	40 hours
Sr. Database Analyst/Programmer	UML, ColdFusion, SQL	Technical	40 hours
Int. Software Developer (2)	UML, Java, ColdFusion, SQL	Technical	40 hours
Int. Systems Analyst/Programmer	UML, Java, ColdFusion, SQL, Testing	Technical	40 hours
Quality Assurance Manager	Quality Assurance, CMMI	Program	20 hours

Table 2-2

Table 2-3 provides the number of support staff hours required as well as the necessary skill set (Skill Category column). The skill category is further defined by whether the skill category is considered technical or program related. The support staff hours are broken down by each skill category. This information will help management determine the resources required and when they are needed.

Position	Skill Category	Technical/Program Related	Staff Hours (avg. per week)
FASS-PH IT Manager	HUD IT program management	Program	40 hours
REAC DBA Team	Database analysis, management, coordination	Technical	8 hours
REAC Integrated Test Team	Testing	Technical	As required for release
Integration/Migration Staff	Migration and integration support	Technical	As required for release
Infrastructure Support	Maintenance of servers, access rights, disaster recovery	Technical	As required

Table 2-3

2.2 Risk Management Structure

Table 2-4 identifies the organizations responsible for managing identified risks and maintaining countermeasures.

HUD Sponsor	Reviews and approves risk databases and mitigation plans, and reviews the status of risk management activities periodically
Project Manager (PM)	Has overall responsibility for mitigating and managing risks
Risk Analysis Peer Group (consisting of project team members, Subject Matter Experts (SMEs) and other appropriate stakeholders appointed by PM)	Each member of the peer group champions a different risk to promote involvement and ownership
Risk Manager	Facilitates risk analysis peer group in this process (may be the PM)
Project Members	Identifies and track risks, participate in, or support, risk analysis peer group
Quality Assurance (QA)	Reviews risk activities, ensures adherence to Risk Management Process
Configuration Management (CM)	Controls risk work products

Table 2-4

2.3 Periodic Risk Assessment

The purpose of this section is to describe the frequency of periodic risk assessments of the operational system as defined by HUD's Software Development Methodology and the required HUD Risk Assessment Template instructions.

The risk assessment objective for this release and subsequent releases is to control the conditions of a task in an effort to prevent risk. This will be done by employing the Software Engineering Institute's definition of the concept, *Continuous Risk Management*.

> Continuous Risk Management is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to: [4]
>
> - Assess continuously what can go wrong (risks).
> - Determine what risks are important to deal with
> - Implement strategies to deal with those risks.

With this framework in mind, risk assessment activities will be performed through out the life of the project.

Preliminary assessments will be conducted at the beginning of the project to identify process, product and constraint sources as well as identify risk categories and specific risk statements within those categories. These preliminary assessments are known as the Software Risk Evaluation (SRE) sessions. The benefit of these sessions is to provide management with an early-warning mechanism for anticipating and addressing project risks.

Upon completion of the Software Risk Evaluation sessions, formal and informal methods will be implemented to track risk to completion at the end of the release. These formal and informal processes in addition to the Software Risk Evaluation sessions are listed in Table 2-5.

[4] *Software Engineering Institute*, "SEI Definition of Continuous Risk Management" (http://www.sei.cmu.edu/programs/sepm/risk/overview.html)

Method	Participants	Method Type	Proposed Coordination Interval
Risk Identification & Analysis Risk Interview	Project Members	Software Risk Evaluation	One time (per individual) at the beginning of the project (Define phase)
Risk Identification & Analysis Session	Risk Analysis Peer Group	Software Risk Evaluation	One time following the conclusion of the Risk Interviews by one week (Define Phase)
Cross-Area Strategy Session	Subsystem Members/ Risk Analysis Peer Group	Software Risk Evaluation	One time following the conclusion of the Risk Identification & Analysis Session by one week (Define Phase)
Interim Report Presentation	Risk Analysis Peer Group	Software Risk Evaluation	One time following the conclusion of the Cross-Area Strategy Session by one week (Define Phase)
Mitigation Strategy Planning Session	Risk Analysis Peer Group	Software Risk Evaluation	One time following the conclusion of the Interim Report Presentation (Define Phase) by one week
Final Report Presentation	Project Management/Risk Analysis Peer Group	Software Risk Evaluation	One time following the conclusion of the Mitigation Strategy Planning Session (Design Phase) by one week
IT Project Review	FASS-PH IT Manager/Contractor Project Members	Formal	Weekly
Business Project Review	FASS-PH Business Team/FASS-PH IT Manager/Contractor Project Members	Formal	Weekly
Contractor Project Review	Contractor Project Members	Informal	Weekly
Meeting Minutes	Contractor Project Members	Informal	Per Meeting
Task Matrix Risk Flags	Contractor Project Members	Informal	Ongoing
Contractor Status Report	Contractor Project Members	Informal	Weekly
Lessons Learned Review	FASS-PH Business Team/ FASS-PH IT Manager/Contractor Members	Formal	One time following the implementation of the release in production (Operate Phase)

Table 2-5

2.4 Contingency Planning

There are two broad types of risk mitigation strategies:

- Preventative – actions planned to reduce the likelihood a risk will occur, and the seriousness if it does occur
- Contingency – actions planned to reduce the seriousness of the risk if it does occur.

This section addresses contingency planning.[5] Contingencies are actions planned to reduce the seriousness of the risk if it does occur. Risks must be monitored and periodically reevaluated. Often more than one tactic may be used. For a risk of potentially high severity, there must be both preventative measures taken to avoid the risk and contingency steps planned for if it should still occur. The guideline for warranting contingency plans is to base the development of these plans on the probability that a risk will evolve into a problem.[6]

After analyzing the potential risks, the PM develops contingency plans to reduce the seriousness of the risk if it does occur. The PM will determine the level of contingency planning needed and identify the responsible personnel involved based on the results of the activities described in this section.

Contingency planning activities are based on the results of the Software Risk Evaluation sessions. This section will cover the purpose of Software Risk Evaluation sessions as they relate to contingency planning. A more detailed explanation is provided in Section 4. The high-level sequences of activities to be executed in developing contingency plans are:

1. Establish criteria warranting the development of contingency plans
1. Identify significant risks during Risk Identification & Analysis that meet or exceed the established criteria
2. Conduct in-depth, structured discussions regarding the sources of these identified risks during the Mitigation Planning session
3. Conduct in-depth, structured discussions regarding potential contingencies for each identified risk during the Mitigation Planning session
4. Select the most effective strategy that will be employed as a contingency for the identified risk
5. Determine the required activities that would support the selected strategies
6. Identify key measures that will be used to track and control executed contingencies
7. Identify possible resources and constraints for suggested strategies
8. Estimate the scope of effort needed

The objective of these activities is to:

[5] Preventative strategies are covered in Section 4.

[6] The difference between a risk and a problem is defined in Section 4.

- Define the contingency plan's goal specific to each identified significant risk
- Identify source of each identified risk requiring a contingency plan
- Select the contingency for each identified risk
- Identify resources responsible for addressing selected strategies
- Determine the budget estimate for executing a contingency plan
- Determine the schedule estimate for executing a contingency plan

To estimate the true effort required to execute a contingency plan, the Project Manager will determine the resource allocations needed, and establish a schedule; the project should break down the activities into tasks. Realistic estimates can be determined only after the tasks to be performed and the actual resources that are available to implement them are delineated. These estimates will be used as a guide when developing contingency plan estimates.

The following considerations will be taken into account when identifying contingency plans:

- The contingency plan goal for a risk does not conflict with the goals of any other risk
- The strategy for a risk does not conflict with the strategy of any other risk
- In the event a strategy for a risk *does* conflict with the strategy of another risk, specific rules for when that strategy will be invoked will be included
- A fully reconciled listing of activities that will be taken in pursuit of these strategies is clearly outlined

With the approval of the GTM, the documented contingency plans will be executed.

3.0 SYSTEM SECURITY

3.0 SYSTEM SECURITY

The following sections are an assessment of the security requirements and specifications necessary to safeguard the system and its corresponding data.

3.1 Baseline Security Requirements

In order to determine the security controls that will be required to adequately counteract security threats, an analysis of the processes and procedures required in Release 8.0 will be conducted at the beginning of the project as well as tracked as part of continuous risk management activities. This identification and analysis will be conducted via the Software Risk Evaluation sessions described in Section 4. There will be a particular focus on the sensitivity of the data that the system will be processing to determine inherent security risks. The key criteria for the baseline security requirements are listed in Table 3-1.

Key Criteria	Detail
Confidentiality	Confidential data must be protected from unauthorized access
Integrity	Data entities must be consistently and comprehensively applied across the database
Accuracy	Data must reflect the business details and objects that they represent
Availability	Data must be available to users with minimal interruption to business processes

Table 3-1

3.2 Baseline Security Safeguards

Analysis will be conducted throughout the project to determine the adequacy of security-related technology that is currently available or scheduled to be made available at the time of release. Safeguard recommendations may be a result of this analysis. Existing baseline security safeguards are listed in Table 3-2.

Existing Safeguard Type	Detail
General User Access	Access to the system is controlled using HUD's Standard Application Security module WASS. This module identifies an individual's ability to access certain functions and data based on their individual functional needs
User ID and Password	WASS requires a unique user ID and password in order to enter the system
Contractor Access	Contractors enter FASS-PH through the WASS security application. Each contractor has a security coordinator that is responsible for managing the organization's use of the WASS system. The coordinator is responsible for supplying authorization to different applications that are available on WASS to each employee in the organization
Internal Employee Access	Internal PIH-REAC employees and Housing employees will obtain unique WASS user ID and password combinations to access the online system. A PIH-REAC technical representative will monitor access similar to access management throughout other PIH-REAC subsystems
Roles and Permission Assignation	The PIH-REAC System Administrator will be authorized to assign FASS-PH roles to internal PIH-REAC users.
HUD's LAN User Access	LAN passwords must be changed periodically
Unauthorized System Access	Unauthorized access is controlled by the application level security Unauthorized users are identified by HUD's Standard Application Security module
Inaccurate/Incomplete Data	Inaccurate and incomplete data is identified and eliminated with extensive up-front edits and the incorporation of precise business rules
Data Corruption/Destruction	As data is entered or modified, system applications perform a variety of validations and FASS-PH displays online help messages as necessary
Deletion of Data	Users cannot directly update or delete data in FASS-PH
Separation of Reporting Functionality	Reports are run against a "mirror" database eliminating reporting functions as a possible source of error
Multi User Processing	The system uses a central database where users access the same data at the same time
Communications	The system uses HUD's Intranet (HUDWeb) to transmit information between Headquarters, Regional Offices, and Program Centers. There is no direct access to the database from the Internet
System and Operational Data Archives	All REAC system data and operational data is archived in parallel database systems in accordance with HUD's IT requirement
Development Environment and Work In Progress Archives	All REAC development environments and work-in-progress is archived in parallel storage systems in accordance with HUD's IT requirements
Restoration of System	All systems can be restored in the event of a failure or a breach in accordance with HUD's IT requirements.

Table 3-2

3.3 Sensitivity Level of Data

An evaluation of the data being processed will be conducted to determine whether the level of sensitivity requires safeguards. An initial assessment has been completed to determine sensitivity levels. Further analysis is required and will be conducted via the Software Risk Evaluation sessions described in Section 4. The initial assessment's results are displayed in Table 3-3. The last column, "Sensitivity Level" represents the result of the initial assessment conducted.

Input/Output	Data Sources	Data Description	Sensitivity Level
Output	HEREMS database/Public Housing Authority (PHA)/PHA roles/Analyst/Managers/Director	Public Housing Authority data	**High**
Output	HEREMS database/ FASS-PH Analyst/Managers/Director	Reviewers Data	**High**
Input & Output	PHA Financial Data Schedule and Data Collection Form	Financial data	**High**
Input & Output	Reviewers	Evaluation data	**Medium**

Table 3-3

The following applicable laws and regulations were considered in our initial assessment and will be referred to in the detailed analysis of data sensitivity issues:

- Privacy Act, 1974, Public Law 93-579, 5 US Code 552a
- Office of Management and Budget Circular A-123 – Directive on Internal Control Systems
- Office of Management and Budget Circular A-127 – Directive on Financial Management of Government Resources
- Computer Security Act of 1987

3.4 User Security Investigation Level and Access Need

Analysis of the system's end users will be conducted to determine who has direct access and specifically who will indirectly receive output from the system. The objective of this analysis will be to determine the levels of security investigation and system access required for each user. The analysis will be conducted via the Software Risk Evaluation sessions described in Section 4. An initial assessment of access requirements has been completed. The results of this assessment follow. The assessment was based on the security requirements of the previous release.

4.0 RISKS AND SAFEGUARDS

4.0 RISKS AND SAFEGUARDS

Risk and opportunity are interrelated. The opportunity for advancement in a software development project cannot be attained without taking risk. Risk is essential to progress and failure is often a key part of learning. The objective in this release and subsequent releases is to balance potential negative consequences of risk against potential benefits associated with opportunity.

The activities associated with Risk Management are described in Table 4-1.

Activity	Description
Identify	Search for and locate risks before they become problems.
Analyze	Transform risk data into decision-making information. Evaluate impact, probability, and timeframe, classify risks, and prioritize risks.
Plan	Translate risk information into decisions and actions (both present and future) and implement those actions.
Track	Monitor risk indicators and mitigation actions.
Control	Correct for deviations from the risk mitigation plans.
Communicate[7]	Provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks.

Table 4-1

Risk Identification

The process of going from the perception of risk to its representation as a risk entity is defined as risk identification.

Risk identification must focus on uncovering risks and not apportioning blame. The results of risk identification must never be used to evaluate the performance of either individuals or their projects. Otherwise, project team members will naturally be reluctant to bring potential risks to the attention of management or project sponsors. The high-level tasks associated with risk identification are:

- Examine each planned activity on a work breakdown structure to uncover potential risks
- Interview subject matter experts
- Review prior risk management activities performed on this project and other similar projects
- Examine project documentation, especially design and requirements specifications

[7] Communication happens throughout all Risk Management activities.

All members of the project team will continually analyze the list of potential risk areas to identify risks specific to the project.

Communication

Communication is an essential element to the success of the project. The PM meets with the project team to determine any potential risks before they happen. The PM is responsible for reviewing the status of all risks with the project team and senior management to determine if changes are needed in priority, measurements, safeguard or contingency plans, or to the baseline criteria used to identify new risks by source. If potential risks become more critical, the PM will notify the GTM, as appropriate, to ensure that possible issues are discussed with the appropriate corrective action.

Software Risk Evaluation

To determine risk identification criteria, communication with the project team is critical. The Software Risk Evaluation (SRE) sessions are a formal structured environment where discussions regarding the definition of risk to the project are established.

An SRE is used to identify and categorize specific project risk statements emanating from product, process, and constraint sources. The project's own personnel participate in the identification and analysis of risk statements, and in the mitigation of risk areas (collections of risk statements that are likely to have common mitigation strategies) facing their own development effort. The SRE has the following attributes.

An SRE provides a project manager with a structured early warning mechanism for anticipating and addressing project risks. It also introduces a set of activities that begins the process of managing risks. These activities can be integrated with existing methods and tools to enhance project management practices.

A list of the sessions with their descriptions is displayed in Table .4-2.

Session	Detail
Risk Identification & Analysis	During the Risk Identification & Analysis (RI&A) session, the Risk Analysis Peer Group meets with the project members (HUD and Contractor) and conducts structured interviews to elicit risk statements. The risk statements are analyzed, prioritized with regard to impact on the project, and grouped into risk areas. The Risk Analysis Peer Group then presents these findings to the Project Manager and FASS-PH IT Manager.
Cross-Area Strategy	The cross-area strategy session identifies conflicts and synergies among the strategies and actions developed for each mitigation area.
Interim Report	During the Interim Report session, the Risk Analysis Peer Group reanalyzes the risk areas and prepares a recommendation of those to be addressed in Mitigation Strategy Planning (MSP) for the Project Manager. This recommendation is agreed to by the Project Manager before proceeding with the MSP session.
Mitigation Strategy Planning	The Mitigation Strategy Planning (MSP) session is focused on the construction of high-level mitigation plans for the selected subset of

	risk areas. Project members, management, and the Risk Analysis Peer Group work together to create goals, strategies, and activities that will mitigate the concerns identified within the risk areas. Project members, now equipped with the necessary information, plans, and sponsorship, can begin mitigating their most critical risks.
Final Report	The mitigation strategy plans are added to the information already compiled and the final report is assembled. The final report and the associated risk data are presented to the FASS-PH IT Manager and FASS-PH Business Manager for final approval.

Table 4-2

To accomplish anything of value, the project itself (and therefore the project manager) must take on risk, and typically faces several major challenges, such as

- New development process
- Technical requirements of the system
- Constraints placed upon the project by the Business or other organizations such as DCG or HUD-IT
- Aggressive budget and schedule

The primary objective is to identify the risks that may affect the project. The data being sought will include:

- Clear “picture of success” for the project in the eyes of the project members
- Issues, worries, and concerns about achieving that picture of success
- Specific conditions existing in the project that are generating those issues, worries, and concerns

Risk Identification & Analysis (RI&A) Session

The heart of the risk management process is the construction of the risk statement in the condition-consequence form, and this construction is accomplished in the interview session.

The two segments of the RI&A Session are listed below with a description of each in Table .4-3.

Segment	Detail
Individual Interview	Project members are asked questions designed to elicit risks within the project. The Risk Analysis Peer Group conducts the interviews, collects context, and captures risk statements put forth by project members.
Group Participation	Project members are asked to individually score the collectively generated risk statements for probability and impact (risk exposure) and then to choose the top five risks to the project

Table 4-3

The risk interview is the basic information-gathering activity of the SRE. Risk interviews are structured interviews of selected key project people, which focus on their individual knowledge of the project risks. The activity brings the participants' knowledge out into the open in a non-threatening way by adhering to the principles of non-attribution and confidentiality. The risk interview generally supports the principle of individual knowledge (i.e., for the most part, risks in the project are known by the individuals working on the project). In general, the risk interview is an engine that creates the fundamental output of the SRE: the risk statement.

The risk statement is the product of the risk interview step and consists of

- Condition: something that is true or accepted as true
- Separator: a semicolon, arrow, or linking phrase
- Consequence: something that may occur as a result of the condition

The SRE uses the Taxonomy-Based Questionnaire (TBQ) to elicit risks from the interview participants. In the Session Analysis step, the Taxonomy is used as a classification framework for risk statements created in the interview.

The taxonomy is a conceptual framework of all the potential sources of risk to the project. This framework considers all the risk sources that are:

- Inherent in or driven by the product the project is creating.
- Associated with the way the project has chosen to go about its development
- Outside the project's control

A specific set of questions will be used for probing into each area of the conceptual framework. These will be written out fully so that different interviewers always ask the same question the same way, and so that the questions can be improved over time.

Risks are elicited and captured during an interview. An interview protocol is used which combines the use of a structured question list and follow-up questioning or "probing" for a potential risk.

During the group participation segment, the classification of all risk statements is revisited in order to create risk areas, which are logical collections of risks that the team feels, can be mitigated as a group.

In the group participation segment, risk exposure of each risk is determined by the group. This is done by associating a score for impact and probability to each risk. These risk exposures are arranged in descending order from those that the team had the most disagreement on to the least. During this sub-step, the team revisits the risks, discussing each and attempting to come to a consensus or to understand why team members scored them as they did. Values that change because of these discussions are revised and re-entered into the team's reconciled scoring worksheet.

Interim Report Session

During the Interim Report phase, the results of the Risk Identification and Analysis (RI&A) session are reanalyzed from the perspective of the interrelationship of the risk areas. The results of the RI&A session

are formally documented, and a recommendation of the risk areas to be addressed in the Mitigation Strategy Planning (MSP) session is made to the Project Manager. An agreement is reached on those risk areas, and the MSP session is scheduled.

The interrelationship digraph is used to discern dependency relationships among the risk areas captured during the RI&A session of the SRE.

Inputs for this include:

- Risk areas, which consist of the area title and the risk statements under it
- Group session context summaries

The output of this activity is the interrelationship digraph, which is useful for illustrating the cause and effect relationship of risk areas. It also helps the Risk Analysis Peer Group to prioritize risk areas for mitigation.

To create an interrelationship digraph the Risk Analysis Peer Group will first examine the risk statements in each risk area for their impacts on other risk areas. These impacts are assigned a weighting and noted on the diagram as outgoing arrows. Next, the Risk Analysis Peer Group will determine the most important effects and the relative direction of the arrows. The result is a cause and effect diagram of risk areas.

A large number of outgoing arrows from one risk area indicate that the area has a causal or influential effect on a number of other risk areas, and it may be a root cause or an item that must be dealt with first. This risk area will be considered as a “Cause/Driver”.

A large number of incoming arrows indicate that the risk area is affected or influenced by a number of other risk areas. This risk area will be considered as a “Result/Rider”.

The *hierarchical* interrelationship digraph is simply a rearrangement of the interrelationship digraph described above to make it tell a more persuasive story. Specifically, the risk areas that are the most significant *drivers* of the other risk areas are moved to the top half of the diagraph, and the risk areas that are the mostly just the *result* of risks in other areas are moved to the bottom half

The interim report forms the basis of the MSP work in the remainder of the SRE. An important document provides:

- Snapshot of the risks facing the project
- Background and discussion surrounding the risk areas and information presented at the data confirmation briefing
- All the risk statements and their risk exposure scores
- Decision-making information to the project manager regarding which risk areas to mitigate first

Mitigation Strategy Planning Session

The Mitigation Strategy Planning (MSP) session begins the strategy to develop a concrete plan for managing and mitigating some of the most important risks identified during the Risk Identification and Analysis (RI&A) session. During the MSP session, project members learn an effective process and a set of methods that can be used to manage identified risks. Metrics that can be used to track risk and mitigation plan progress are identified, and plans are made for evaluating the success of the mitigation strategies.

Possible mitigation strategies often occur to Risk Analysis Peer Group members before the MSP session. A suggestion may have been made during the RI&A session, or an area may seem similar to one addressed during a prior SRE. Such approaches can be shared during the MSP session to get the ball rolling or contribute a good idea that should be considered.

During MSP session, in-depth, structured discussions of each mitigation area are conducted. The goal of these sessions is to begin to identify and document how the risk areas might be mitigated. The depth of planning in an MSP session is dependent on the group problem-solving skills of the project members who have been assembled. If this is a completely unfamiliar process for them, or if the junior members of the group are unable to participate fully in the company of their superiors, it can take a long time to achieve full participation.

The items for discussion in the MSP session include:

- Discussing and identifying possible causes of the risks
- Discussing and identifying mitigation goals for the risks
- Discussing and determining possible mitigation strategies
- Discussing and determining mitigation activities that would support suggested strategies
- Beginning to identify key measures that will be used to track and control mitigation activities
- Discussing possible resources and constraints for suggested strategies
- Estimating the scope of effort needed

The inputs to the MSP session include:

- Mitigation areas that have been determined and agreed upon
- Roles and assignments that have been determined for conducting the session
- Schedule for MSP session

For each risk area addressed, outputs of the MSP sessions should include:

- Mitigation goal specific to the risk area
- Sources of the conditions of the risk statements for the risk area

- Strategies
- Supporting actions for those strategies
- Metrics
- Budget estimate
- Schedule estimate
- Actions, metrics, and goals that are linked to schedule and project milestones

Each participant in the session will be given a chance to discuss the area and possible causes of the risks in it. The goal is for everyone involved to understand the risk area and the alternatives being considered. Ideas should be shared and discussed openly.

To estimate the true effort required to mitigate a risk area, the Project Manager will determine the resource allocations needed, and establish a schedule; the project should break down the activities into tasks. Realistic estimates can be determined only after the tasks to be performed and the actual resources that are available to implement them are delineated. The individuals responsible for implementing the plans can use these estimates as a guide. However, final documentation of plans will not be conducted until the conclusion of all on-site activities. The outcome of the cross-area strategy session, described in the next section, may result in changes to individual mitigation plans.

The session will have the following key results for each risk area addressed:

- Mitigation goal for the risk area which does not conflict with the goals of any other risk area
- Set of mitigation strategies to pursue that does not conflict with that of any other risk area. (If it does, specific rules for when that strategy will be invoked will be included
- Fully reconciled listing of activities that will be taken in pursuit of these strategies

The MSP results briefing is a formal presentation in which all of the MSP participants see the results of the overall mitigation plan, and learn how their own planning efforts contributed to these results. Project members are shown how the risk areas addressed in the MSP session will be mitigated.

The MSP results briefing enables the identification of the appropriate next steps, such as

- Getting required authorizations, contract modifications, or approvals
- Defining needs for more detailed plans
- Clarifying cost and personnel estimates
- Determining the frequency of data collection, evaluation, and reporting
- Establishing the means by which to report status

The input data from the Software Risk Evaluation sessions will be stored in a Risk Database. This allows the project members to build a continuous risk management process into each release. The database will be built and tailored to suit the needs of the project. The types of data that will be entered are:

- Risk statements
- Context
- Evaluations of the individual risks for impact and probability
- Classification of risk statements into risk areas
- Prioritization of the individual risk statements
- Mitigation strategies
- Responsible individuals
- Mitigation plans in the form of action items.

Cross-Area Strategy Session

The cross-area strategy session identifies conflicts and synergies among the strategies and actions developed for each mitigation area. Conflicts and synergies among strategies often occur when MSP sessions are conducted by parallel teams or when different people are involved with each session. Conducting a cross-area strategy session minimizes the potential for conflicting plans or duplicated effort, and maximizes the impact of strategies, resources, and actions.

The activities associated with the Cross-Area Strategy session are:

- Reviewing mitigation area results
- Identifying conflicts, commonalities, dependencies, and possible sequencing
- Resolving conflicts
- Prioritizing strategies and actions
- Reviewing and closing out the cross-area strategy session
- Documenting the overall mitigation plan which can be completed offline or in parallel with the MSP results preparation activities
- Reconciling individual risk area plans

The objective of the Cross-Area Strategy session is to improve mitigation strategies and actions from each risk area by adding aplicable strategies and actions that came out of the Cross -Area Strategy session.

This session is conducted as a problem-solving and decision-making activity, in which methods such as brainstorming and structured facilitation should be used.

The cross-area strategy session is optional and may not be necessary if the mitigation areas are clearly unrelated with no overlap in strategies and actions.

Before determining whether a cross-area strategy session is needed, the Risk Analysis Peer Group will review all mitigation plans to check for potential conflicts and synergies. Mitigation area prioritizing that result from the MSP planning meeting will be revisited at the conclusion of the MSP session.

Risk Statement

For a risk to be understandable, it must be expressed clearly. The Risk Statement should include:

- A description of the current conditions that may lead to the loss
- A description of the loss

The project team will use the condition-transition-consequence (CTC) based approach for risk identification and management activities. This will allow the team to establish a distinct risk entity that represents the true meaning of risk.

The definition of risk that we will base our activities on is that a risk involves a condition that has a noticeably adverse effect on the program currently, but also is perceived to indicate additional and/or more serious problems in the future.

A sense of risk is present as long as there is a perception that the current circumstances may result in loss. For the purposes of software development risk identification, risk is minimally considered as the description of the current condition and a sense of potential loss. This sense of loss may be presented as a notional description of the potential consequence. That is, the current circumstances will result in a continuous sequence of events so that at some point the evolution of the project results in inability to meet its overall objective.

There is often an issue relating to whether a situation (condition) is a problem or a risk. A problem involves a value judgment made upon the merits of the current condition. It is a condition that exists and is undesirable. A risk involves a value judgment made upon the potential implications of the current condition. It suggests a possible, future undesirable condition (consequence).

It is important to understand the difference between a “problem” and a “risk”. Confusion between the two terms is common. A problem is an existing condition that has adverse attributes. The loss associated with a problem is evident in its description of the condition (problem). When the condition is described, the negative aspects are evident and undesirable circumstances currently exist. Many problems are risks in that they may lead to symptoms that are more serious or other problems.

The difference between a problem and a risk is the degree that the project is being adversely affected. Risks can evolve into problems and the prevention of this evolution is the heart of risk management.

A risk can be described as a construct consisting of a description of the initial state of the project (condition), the potential evolution of the project (transition), and the potential final state (adverse in

nature) of the project (consequence). The definition of the components of the Condition-Transition-Consequence construct is listed in Table 4-4.

Component	Definition
Condition	Description of current conditions causing concern
Transition	Component that involves change of the conditions (time)
Consequence	Description of the potential outcome

Table 4-4

Many project characteristics can be used to express value in the context of software development. Given that time and value are fundamental to the description of risk, the minimum information needed to identify a risk is the statement of the conditions joined with an expression of concern about the potential consequences.

The undesirable end state does not need to be explicitly stated and the details of the transition do no necessarily need to be specified. The minimal statement is sufficient to risk identification and provides the starting point to initiate subsequent steps in the risk management process. Many times valuable time is wasted on trying to state the risk so specifically instead of addressing the more important question of how to prevent it. That is not to say that any CTC risk statement component itself can be left out of the risk statement. Each component is vital to the supporting successful risk management activities. Attributes of the CTC risk statement are the appropriate elements to utilize when providing specific information about a risk. This level of specificity should not be in the risk statement itself.

An example of a CTC risk statement would be:

- **Given that** *condition* **then there is concern that (possibly)** *consequence.*

The concept of a CTC risk statement includes a descriptive attribute-value set. The attributes are the characteristics of risk such as probability, impact, risk exposure, timeframe information, metrics for tracking and control, as well as administrative information that provide important details on the risk. Collectively, the attribute set and associated values include all of the relevant detail on the nature of a specific risk statement that is required to fully understand and manage that risk. The template for a risk statement with attribute-value set is presented in Table 4-5.

Element	Detail	
RISK STATEMENT	**Given that** *condition* **then there is concern that (possibly)** *consequence.*	
Context (Details on condition relating to risk)		
RISK ATTRIBUTES	**Risk Exposure Rating**	
	Probability Rating	
	Impact	
	Timeframe	
	Metrics	
	Administrative	

Table 4-5

The CTC risk statement allows for the possibility that a single condition has multiple consequences. There are two variations of how this happens. A description of these variations is listed in Table 4-6.

Variation	Detail
Co-occuring	Consequences that occur at the same time
Cascade	Consequences that are considered serial outcomes

Table 4-6

Multiple consequences can be included as part of the scenario attribute of the CTC risk statement. The scenario set describes in more detail the potential evolution of the risk based upon the stated condition. Scenarios provide detail on the transition aspects of the CTC risk statement. The scenario set will be generated as needed. Particular caution will be taken when developing these scenario types to avoid "analysis paralysis".

Relationship to Tasks

Task statements can generally be expressed in the same construct as risks. Specifically a task is expressed in terms of activities needed to achieve an outcome.

Tasks are also described in terms of transition and value. The identified result is a desired result. The activities comprising the task accomplish the transition to the desired result. As work on a task is completed, the project progresses until all the desired consequences are achieved. Therefore, the CTC construct can also be applied to describing a task. This is very helpful in maintaining traceability of risk to project activities throughout the life of the project.

A task is a potential transition from the current state of the project to some other desirable state. For a risk,the emphasis is on the condition whereas with a task the condition is often implicit.

As the planning effort and the project evolve, existing tasks can be decomposed into other tasks. Similarly, risks can be expanded into other risks and additional tasks can be created because of the existence of the risk.

Tasks like monitor, observe, and review may have an implied consequence statement. In this case, the consequence state may be defined by the criteria establishing when the task is completed. Thus, while most tasks emphasize the consequence, the transition description can be more important in a task statement than in a risk statement.

The relationship between tasks and risks for this project will be considered a critical source of information in the Risk Identification & Analysis session.

Project ambiguities are generally a consequence of one of the following:

- Inability to measure or describe the circumstances associated with risk
- Inability to control the highly dynamic characteristics and environment of a software development project.

With the explicit identification of a risk and its attribute-value set, risks can be analyzed, tracked, and controlled as part of Continuous Risk Management (CRM).

Risk Source

Classification is a consensus activity.

The issue regarding whether the condition can be viewed as a “source of risk” relates to an assessment of cause. In many cases, the condition *can* and *is* identified as the source (cause) of the consequence.

To say that a condition is a source (cause) of the risk requires not only that the circumstances be described but also the perception that they may lead to negative consequences. From this perspective, the source as defined above is an integral part of risk and pragmatically is a key defining element of a risk.

Particular caution will be used when identify risk source to avoid confusion and misunderstanding of what constitutes a source of risk. That is, to avoid stating that the conditions cause the possibility of risk. This sidesteps the critical perception issue relative to value. There is a cause-effect relationship between the time now (condition) and what may occur in the future (consequence). There is also a causal relationship between the condition and the sense of concern, doubt, anxiety, or uncertainty, etc. Collectively these causal relationships are involved with risk and are integral to risk and the definition of a risk in the model.

While risk identification should be thorough, it should not attempt to address every potential event regardless of how unlikely it would be to occur. During the initial risk identification process the team will concentrate on identifying the source of certain risks and from these a pattern can be established to help predict the likelihood of its occurrence. The risk categories derived from this process will constitute a baseline of risks from which to begin a more thorough investigation of risks in an ongoing iterative process. This baseline will be revisited whenever new categories of risks are uncovered.

Risk Impact

Particular attention will be made to risks associated with a potential impact to cost and schedule or system performance. Risks documentation must include the context, conditions and potential consequences of the risk should it materialize.

The following table is a list of the impact ratings that will be used for the project.

Impact	Detail	Rating
Minor	Insignificant impact	1
Marginal	Will reduce performance but is not a source of irritation	2
Serious	Will reduce performance but is a source of irritation	3
Critical	Project is adversely impacted; Fix or Re-work of process is likely	4
Catastrophic	Complete failure	5

Table 4-7

Risk Probability

The following table is a list of the probability ratings that will be used for the project.

Probability	Detail	Rating
Not likely	Self-explanatory	1
Documented low failure rate	Historical evidence of low probability is documented	2
Undocumented low failure rate	Historical evidence of low probability is believed by project members but no documentation exists	3
Failure occurs from time to time	Self-explanatory	4
Documented moderate failure rate	Historical evidence of moderate probability is documented	5
Undocumented moderate failure rate	Historical evidence of moderate probability is believed by project members but no documentation exists	6
Documented high failure rate	Historical evidence of high probability is documented	7
Undocumented high failure rate	Historical evidence of high probability is believed by project members but no documentation exists	8
Failures Common	Self-explanatory	9
Failures nearly always occur	Self-explanatory	10

Table 4-8

Risk Priority

Priority is based on risk exposure. Risk exposure is a measure used during the analysis portion of the RI&A session and is created by combining the impact and probability of the risk, should it materialize.

Risk Detectability

The goal of Continuous Risk Management is to provide early detection of risk to the Project Manager. Detection of risk is also rated for measurement purposes and is especially telling when conducting post-mortems after the completion of a project. The following table is a list of the detectability ratings that will be used for the project.

Detectability	Detail	Rating
Nearly certain to detect before production	($p \approx 0$)	1
Extremely low probability of reaching production without detection	($0 < p \leq 0.01$)	2
Low probability of reaching production without detection	($0.01 < p \leq 0.05$)	3
Likely to be detected before reaching production	($0.05 < p \leq 0.20$)	4
Might be detected before reaching production	($0.20 < p \leq 0.50$)	5
Unlikely to be detected before reaching production	($0.50 < p \leq 0.70$)	6
Highly unlikely to be detected before reaching production	($0.70 < p \leq 0.90$)	7
Poor chance of detection	($0.90 < p \leq 0.95$)	8
Extremely poor chance of detection	($0.95 < p \leq 0.99$)	9
Nearly certain that failure won't be detected	($p \approx 1$)	10

Table 4-9

Risk Analysis

Project ambiguities are generally a consequence of one of the following:

- Inability to measure or describe the circumstances associated with risk
- Inability to control the highly dynamic characteristics and environment of a software development project.

With the explicit identification of a risk and its attribute-value set, risks can be analyzed, tracked, and controlled as part of Continuous Risk Management.

The objective of Risk Analysis is to successfully execute the following tasks:

- *Risk Assessment* (figuring out what the risks are and what to focus on) [8]
    - Making a list of all of the potential dangers that will affect the project
    - Assessing the probability of occurrence and potential loss of each item listed
    - Ranking the items (from most to least dangerous)

[8] *Introduction to Risks in Software Project Management (http://www.baz.com/kjordan/swse625/intro.html)* April 24, 1997

- *Risk Control* (doing something about them)
    - Coming up with techniques and strategies to mitigate the highest ordered risks
    - Implementing the strategies to resolve the high order risks factors
    - Monitoring the effectiveness of the strategies and the changing levels of risk throughout the project

One of the keys to successful project execution is a practical measurement, tracking, and forecasting framework. The framework needs to provide early warning so that leaders can better understand what's happening on their project and take appropriate actions.

Everyone on the project must be committed to and participate in the collection of an adequate set of measurement data; however, there is a delicate balance between having enough information and drowning the developers with overwhelming data requirements. The challenge is to find the right balance where everyone benefits.

The following key project indicators should at minimum be addressed in this effort:

- Project Cost
- Project Schedule
- Product Quality and Reliability

The CTC risk statement provides a starting point in determining what metrics should be collected for analysis because it is characterized by both descriptive and measurable attributes that capture the essential elements of risk, and that relate, directly or indirectly, to factors critical to successful project management, e.g. budget, performance, and schedule.

Measurements will be collected and tracked to determine if risks are being prevented, minimized, or have occurred. These measurements will be documented in the Final Report of the Software Risk Evaluation sessions.

Risk Tools

There are a number of risk management tools that can be used to store risk information, evaluate risks, track status of risk items, and generate reports or charts depicting risk management activity. Risk Management tools are vital to the success of risk analysis initiatives.

One of the tools that will be used for this release and subsequent releases is the task matrix. The task matrix is a spreadsheet listing all the project tasks. Each task is measured (when feasible) for timeliness, age, reliability, external dependencies, and level of effort. Critical path tasks have been defined in this task matrix and the timeliness of these tasks is crucial to the success of the project. For example, the task that addresses Business sign-off on the requirements must happen by the end of the Define phase. The adverse consequence of this not happening in the acceptable timeframe is that requirements are not concrete for the follow-on task of designing for the requirements.

This has a cascade affect of negative impacts on the project schedule. If this task does not happen within the acceptable timeframe a risk flag is auto-attached to the task when the completion date exceeds the due date and/or the status does not equal 100% by the due date. Tasks with risk flags are added to the risk matrix for tracking and potential action by management. For additional use of tools, Avineon will work with HUD to determine which tool may be the most beneficial to the HUD's environment to effectively manage and mitigate risks on the project.

Risks

The following is a list of potential risks associated with project planning, monitoring, and management including their categories, impact ratings, probability ratings, and risk exposure ratings. Mitigation strategies are a result of the Software Risk Evaluation sessions and are not listed below. These are *not* necessarily specific risks to the project. True project-related risks are a result of the Software Risk Evaluation sessions and subsequent identification procedures described above that happen during the various phases of the project.

Risk ID	Category	Risk	Impact	Probability	Risk Exposure
1	Project Planning	Given that critical computer resources were not identified than there is a concern that possibly the hardware required will not be received at all or in the acceptable time frame for the successful implementation of the project objective	5	8	40
2	Project Management	Given that data was not available for the selected measure for the sub process than there is a concern that possibly the selected measure will not be useable.	4	8	32
3	Project Management	Given that no statistical and quality management data was recorded or stored for the prior release than there is a concern that defining required measures will take longer than anticipated.	4	8	32
4	Project Monitoring and Control	Given that the status of stakeholder involvement was not reviewed periodically than, there is a concern that possibly, the stakeholder commitments will not be met.	4	8	32
5	Project Monitoring and Control	Given that significant issues regarding stakeholder involvement were not documented than, there is a concern that possibly, commitment to the project plan will not be obtained.	4	8	32

6	Project Planning	Given that the estimate of critical computer resources was not based on allocated requirements than there is a concern that possibly the critical computer resources will not be received or not received in an acceptable time frame for the successful implementation of the project objective.	4	8	32
7	Project Planning	Given that the equipment requirements were not defined than there is a concern that possibly the necessary equipment will not be made available in time to complete the tasks.	4	8	32
8	Project Monitoring and Control	Given that the commitments were not reviewed with the team than there is a concern that possibly the commitments will not be met.	4	7	28
9	Project Management	Given that measures from the organizational process assets were not identified than, there is a concern that possibly the statistical management of the sub processes cannot be supported.	3	8	24
10	Project Planning	Given that the work packages were not identified in sufficient detail then there is a concern that possibly the project tasks, responsibilities and concerns were not estimated properly.	3	8	24
11	Project Planning	Given that commitments were not adequately negotiated than there is a concern that possibly, the requirements will not be signed off.	4	6	24
12	Project Management	Given that statistical management criteria was not considered when sub processes were identified, than there is a concern that possibly the sub process are not suitable for statistical management.	3	7	21
13	Project Management	Given that the selection criteria for sub processes were not identified than there is a concern that possibly, the required areas of predictable performance will not be satisfied.	3	7	21
14	Project Management	Given that the defect density of the sub process was not identified than there is a concern that possibly, the sub process cannot be controlled sufficiently.	3	7	21

15	Project Management	Given that the operational definitions of the measures were not specified, regarding communication than there is a concern that possibly vital information regarding the measures will not be reported.	3	7	21
16	Project Monitoring and Control	Given that the resources used were not monitored than, there is a concern that possibly, the resources used will exceed the resources allocated in the project plan.	3	7	21
17	Project Planning	Given that the work products that will be externally required were not identified than there is a concern that possibly these work products will not be received at all or not received within the acceptable timeframe to receive these work products.	3	7	21
18	Project Planning	Given that risks were not identified at the beginning of the project than there is a concern that possibly, the work efforts could be negatively impacted with no recourse available.	3	7	21
19	Project Planning	Given that the identified risks were not documented than, there is a concern that possibly, the risks will not be sufficiently mitigated.	3	7	21
20	Project Planning	Given that the risk was not revised, following stakeholder's input than there is a concern that possibly the risk will not be mitigated sufficiently.	3	7	21
21	Project Management	Given that the sub process' capability deficiencies were not documented than there is a concern, that possibly no corrective action will be implemented.	4	5	20
22	Project Monitoring and Control	Given that changes to external commitments were not negotiated effectively than there is a concern that possibly, the projected schedule will be impacted by the misalignment of design tasks.	4	5	20
23	Project Planning	Given that the WBS was not based on the current project/product architecture then there is a concern that possibly, the work described in the WBS will not support the project's objectives.	5	4	20

24	Project Planning	Given that stakeholder's agreement was not obtained regarding the documented risks than there is a concern that possibly a risk will not be sufficiently mitigated.	4	5	20
25	Project Planning	Given that commitments regarding interfaces with other subsystems were not identified than, there is a concern that possibly, these commitments cannot be monitored sufficiently and validated.	4	5	20
26	Project Management	Given that special causes of variation were not identified than there is a concern that possibly the complexity of classifying a variation will be insurmountable.	3	6	18
27	Project Management	Given that the special causes of process variation were not analyzed than there is a concern that possibly, the reason the anomaly occurred will remain unknown.	3	6	18
28	Project Management	Given that the changes in quality and process-performance objectives were not monitored than there is a concern, that the selected sub processes' capability will not be adequate in supporting the objectives.	3	6	18
29	Project Monitoring and Control	Given that the results of collecting and analyzing measures were not reviewed than there is a concern that possibly, the project control will not be adequate.	3	6	18
30	Project Monitoring and Control	Given that project issues were not collected for analysis than there is a concern that possibly, the issues will not be accounted for in risk management activities.	3	6	18
31	Project Monitoring and Control	Given that the appropriate actions needed to identify an issue were not documented properly, than there is a concern that possibly, the issue will not be addressed appropriately and will remain open.	3	6	18
32	Project Management	Given that the project's quality and process-performance objectives were not reviewed periodically than there is a concern that possibly the status of these objectives in the project plan is not accurate.	2	8	16

33	Project Management	Given that the project's quality and process-performance objectives were not revised as necessary than there is a concern that possibly the objectives will be compromised.	2	8	16
34	Project Management	Given that the risk of the unavailable sub process was not identified than, there is a concern that possibly, the quality and process-performance objectives will not be satisfied.	4	4	16
35	Project Management	Given that the actual results achieved against the established interim objectives were not reviewed at the end of each phase than there is a concern that possibly the status of the project's quality and performance-objectives is not accurate.	2	8	16
36	Project Management	Given that process-performance models were not calibrated with obtained measures of critical attributes than there is a concern that possibly estimation of progress toward achieving the project's quality and process-performance objectives will not be done appropriately.	2	8	16
37	Project Management	Given that the sub processes did not have suitable historical performance data than there is a concern that possibly natural bounds for that sub process cannot be established.	2	8	16
38	Project Management	Given that the natural bounds were not recalculated after incremental improvements to the sub process than there is a concern that data for this sub process will be inaccurate.	2	8	16
39	Project Management	Given that the quality and process performance objectives were not compared to the natural bounds of the measured attribute than there is a concern that possibly capability of the process will be unknown.	2	8	16
40	Project Monitoring and Control	Given that the actual training obtained by the staff was not monitored than there is a concern that possibly, the required skill set to implement the requirement will not be adequate.	2	8	16

41	Project Monitoring and Control	Given that the data management activity reviews were not documented than there is a concern that possibly, the project plan will not be revised accordingly.	2	8	16
42	Project Monitoring and Control	Given that the results of the stakeholder involvement reviews were not documented than there is a concern that possibly, the project plan will not be revised accordingly.	2	8	16
43	Project Planning	Given that the knowledge and skills needed to perform the project were not identified than there is a concern that possibly the existing knowledge base and skill set will not be adequate to implement the requirement.	4	4	16
44	Project Planning	Given that the mechanisms necessary to provide knowledge and skills to the staff were not selected than there is a concern that possibly the staff will not receive the required training.	2	8	16
45	Project Planning	Given that training was not incorporated in the project plan than there is a concern that possibly the training required would not be received.	2	8	16
46	Project Management	Given that the organization’s objectives were not reviewed for quality and process performance than there is a concern that possibly, the project's objectives for quality and process performance are not within the context of the overarching organization's objectives.	3	5	15
47	Project Management	Given that process performance measurement criteria were not identified than, there is a concern that possibly, the process performance will not meet the required levels of customer acceptance.	3	5	15
48	Project Management	Given that the criteria used to identify which sub processes are valid candidates for use was not established than there is a concern that the overarching quality and process-performance objectives will be compromised.	3	5	15

49	Project Management	Given that the actions needed to address deficiencies in achieving the project's quality and process-performance objectives were not documented than there is a concern that possibly the required corrective action will not be implemented.	3	5	15
50	Project Management	Given that the natural bounds were not calculated for each measured attribute of the sub process than there is a concern that possibly any potential variation will not be identified.	3	5	15
51	Project Monitoring and Control	Given that the project's actual costs was not monitored than there is a concern that possibly the actual costs will exceed the project budget	5	3	15
52	Project Monitoring and Control	Given that the documented risks were not reviewed periodically than there is a concern that possibly, the current-status of the project is not accurate.	3	5	15
53	Project Monitoring and Control	Given that the documented risks were not revised, as additional information was made available than there is a concern that possibly, the risks will not be mitigated.	3	5	15
54	Project Monitoring and Control	Given that the risks were not communicated to the relevant stakeholders than there is a concern that possibly, the mitigation strategy will not be executed as intended.	3	5	15
55	Project Monitoring and Control	Given that project issues were not analyzed than there is a concern, that possibly necessary corrective action for these issues will not be addressed.	3	5	15
56	Project Monitoring and Control	Given that corrective action was not monitored for completion than there is a concern that possibly, the corrective action was not implemented accordingly.	3	5	15
57	Project Monitoring and Control	Given that the results of the corrective action were not analyzed than, there is a concern that possibly, the implemented corrective action was not effective.	3	5	15

58	Project Monitoring and Control	Given that appropriate actions to correct deviations from planned results were not documented than there is a concern that possibly the allocated resources will not meet the necessary resources to implement the appropriate actions.	3	5	15
59	Project Planning	Given that historical data was not used in the estimation of hours and costs for the project than there is a concern that possibly the estimated hours and costs will not satisfy the needs of the project in order to fulfill its objective for this release.	3	5	15
60	Project Management	Given that the interaction of sub processes was not analyzed than there is a concern that possibly the relationship between the sub processes and the measured attributes of the sub processes will not be understood.	2	7	14
61	Project Management	Given that the sub processes were not selected for statistical management using the selected criteria than there is a concern that possibly, the sub processes will not meet the required quality and process-performance objectives.	2	7	14
62	Project Management	Given that the performance of each sub process was not reviewed periodically than there is a concern that possibly the progress toward achieving the project's quality and process-performance objectives cannot be quantified.	2	7	14
63	Project Management	Given that coverage and efficiency of peer reviews for this sub process were not identified as a required measure than there is a concern that the sub process will not support the project's quality and process-performance objectives.	2	7	14
64	Project Management	Given that the relationship of identified measures to the organization's and project's objectives was not properly analyzed than there is a concern that possibly the specific target measures or ranges to be met will not be satisfied.	2	7	14

65	Project Management	Given that the measures and statistical analysis techniques were not revised when necessary than there is a concern that the measures will not support the project's quality and process-performance objectives.	2	7	14
66	Project Monitoring and Control	Given that the measurement of actual completion of tasks was not done than there is a concern that possibly a deliverable will be missed.	2	7	14
67	Project Monitoring and Control	Given that significant deviations in the project plan were not documented than there is a concern that possibly, the status of the project plan will not be accurate.	2	7	14
68	Project Management	Given that traceability of the project's quality and process-performance objectives was not established from their sources than there is a concern that possibly these objectives will not be satisfied.	2	6	12
69	Project Management	Given that the quality and process-performance objectives were not identified for statistical management than there is a concern that possibly, the required statistical management activities will not address the appropriate objective.	2	6	12
70	Project Management	Given that required additional measures specific to this instance of a sub process were not identified than there is a concern that possibly the sub process will not be adequately covered by statistical management.	2	6	12
71	Project Management	Given that the corrective action was not identified for the special causes of variation than there is a concern that possibly a problem will surface.	3	4	12
72	Project Management	Given that the actions needed to address sub process capability deficiencies were not documented than there is a concern that possibly the deficiencies were not addressed appropriately.	3	4	12
73	Project Monitoring and Control	Given that the attributes of the work products were not monitored than, there is a concern that possibly, the tasks deviate from the project plan.	3	4	12

74	Project Monitoring and Control	Given that significant issues and deviations regarding project reviews were not documented there is a concern that possibly the project plan status is not accurate.	2	6	12
75	Project Monitoring and Control	Given that change requests and problem reports were not tracked to closure than there is a concern that possibly, the corrective action necessary was not completed.	3	4	12
76	Project Planning	Given that the number of functions for the work product were not identified than there is a concern that possibly the LOE's provided will not accurately reflect the work needed to implement the requirement	4	3	12
77	Project Planning	Given that the volume of data for the work product were not identified than there is a concern that possibly the LOE's provided will not accurately reflect the work needed to implement the requirement	3	4	12
78	Project Planning	Given that work product attributes were not analyzed sufficiently than there is a concern that possibly the task duration estimated does not provide adequate time to execute the task	2	6	12
79	Project Planning	Given that criteria was not established to determine what constitutes a significant deviation from the project plan than there is a concern that possibly the problems that occur during the project will not be corrected when necessary.	2	6	12
80	Project Planning	Given that requirements for security of data were not established than, there is a concern that possibly the actual required security for the data will not be satisfied.	4	3	12
81	Project Planning	Given that mechanisms for data archival were not established than there is a concern that possibly the data archival will not be sufficient.	3	4	12
82	Project Planning	Given that the current knowledge and skills of the staff were not assessed than there is a concern that possibly the existing knowledge base and skill set will not meet the required knowledge base and skill set for the project.	3	4	12

83	Project Planning	Given that associated plans (other than the project plan) were not reviewed, than there is a concern that possibly, the activities listed in these plans will not be accounted for in the project.	4	3	12
84	Project Planning	Given that organizational commitments were not documented than, there is a concern that possibly, commitments will be forgotten.	3	4	12
85	Project Planning	Given that internal commitments were not reviewed with senior management than there is a concern that possibly decisions made by senior management will be counterproductive.	2	6	12
86	Project Management	Given that the measurable quality and process performance criteria were not documented than there is a concern that possibly, the reports submitted to the customer will be inadequate.	2	5	10
87	Project Management	Given that interim objectives were not derived for each phase than there is a concern that possibly, the quality and process-performance progress is not accurately monitored.	2	5	10
88	Project Management	Given that alternative objectives and long-term objectives conflicts were not resolved than there is a concern that possibly the long-term objectives will be compromised.	2	5	10
89	Project Management	Given that risks associated with achieving the project's quality and process-performance objectives were not identified than there is a concern that possibly the associated risks will not be mitigated.	2	5	10
90	Project Management	Given that the expected statistical analysis techniques were not identified than there is a concern that possibly, the technique employed is not appropriate for the measure collected.	2	5	10
91	Project Monitoring and Control	Given that status was not communicated to the relevant stakeholders than there is a concern that possibly, the stakeholders will not support future tasks.	5	2	10
92	Project Monitoring and Control	Given that the milestone status was not reviewed than there is a concern that possibly the milestones were not achieved.	5	2	10

93	Project Planning	Given that appropriate methods were not used to determine the attributes of the work products and tasks than there is a concern that possibly the estimation of resource requirements is not accurate.	2	5	10
94	Project Planning	Given that the models necessary to estimate labor hours and costs were not used than there is a concern that possibly the estimated hours and costs will not satisfy the needs of the project in order to fulfill its objective for this release.	2	5	10
95	Project Monitoring and Control	Given that commitments that have not been satisfied have not been identified than there is a concern, that possibly corrective action is not executed.	3	3	9
96	Project Monitoring and Control	Given that data management activities were not monitored periodically than there is a concern that possibly these activities will deviate from the project plan.	3	3	9
97	Project Monitoring and Control	Given that significant issues regarding data management were not documented than there is a concern that possibly, these issues will not be addressed appropriately.	3	3	9
98	Project Planning	Given that the source lines of code for the work product were not identified than there is a concern that possibly the LOE's provided will not accurately reflect the work needed to implement the requirement	3	3	9
99	Project Planning	Given that the number of classes and objects for the work product were not identified than there is a concern that possibly the LOE's provided will not accurately reflect the work needed to implement the requirement	3	3	9
100	Project Planning	Given that the number of product requirements for the work product were not identified than there is a concern that possibly the LOE's provided will not accurately reflect the work needed to implement the requirement	3	3	9

101	Project Planning	Given that the number of interfaces for the work product were not identified than there is a concern that possibly the LOE's provided will not accurately reflect the work needed to implement the requirement	3	3	9
102	Project Planning	Given that the number of technical risks for the work product were not identified than there is a concern that possibly the LOE's provided will not accurately reflect the work needed to implement the requirement	3	3	9
103	Project Planning	Given that critical competencies and roles needed to perform the work were not estimated for effort and cost than there is a concern that the critical competencies and roles will not be adequate to successfully implement the customer's requirements	3	3	9
104	Project Planning	Given that schedule assumptions regarding duration were not identified than there is a concern that possibly there are an unknown number of uncertainties in the overall schedule.	3	3	9
105	Project Planning	Given that the estimated and available resources were not reconciled than there is a concern that the project objectives will not be satisfied.	3	3	9
106	Project Management	Given that the customer's priorities were not identified than, there is a concern that possibly, the tasks will not reflect the customer's priorities.	4	2	8
107	Project Management	Given that the capabilities of the organization's support environment were not defined than there is a concern that possibly the collection, derivation, and analysis of statistical measures will not be adequate.	2	4	8
108	Project Monitoring and Control	Given that milestone reviews were not conducted with relevant stakeholders than there is a concern that possibly the status details of these milestones is unknown to the relevant stakeholders.	4	2	8
109	Project Monitoring and Control	Given that relevant stakeholder agreement was not obtained for corrective action than there is a concern that possibly, the budget necessary to execute the corrective action will not be available.	4	2	8

110	Project Planning	Given that the labor required by the project was not estimated than there is a concern that possibly the allocated labor will not fulfill the needs to implement the requirement	4	2	8
111	Project Planning	Given that infrastructure requirements were not considered when estimating effort and cost than there is a concern that possibly the estimated effort and cost is not accurate and will not be adequate to satisfy the project objectives for this release.	4	2	8
112	Project Planning	Given that the project data to be identified and collected were not determined than there is a concern that possibly the project data necessary to track the project's success will not be available.	2	4	8
113	Project Planning	Given that staffing requirements were not defined than there is a concern that possibly, the tasks will not be completed.	4	2	8
114	Project Monitoring and Control	Given that the action items resulting from the milestone reviews were not documented than there is a concern that possibly the project plan was not revised accordingly.	3	2	6
115	Project Monitoring and Control	Given that the action items were not tracked to closure than there is a concern that possibly the action items were not complete.	3	2	6
116	Project Monitoring and Control	Given that the significant issues regarding milestones were not documented than there is a concern that possibly these issues will not be addressed.	3	2	6
117	Project Planning	Given that the technical approach for the project was not defined than, there is a concern that possibly the decisions for architectural features will not satisfy the customer's requirements.	3	2	6
118	Project Planning	Given that the critical path for task dependencies was not defined than there is a concern that possibly the project schedule will slip.	3	2	6

119	Project Planning	Given that the expected availability of resources was not defined than there is a concern that possibly the resources allocated to the task will not be available in time to complete the task	3	2	6
120	Project Planning	Given that the process requirements were not identified than there is a concern that possibly the efficient operations during project execution cannot be guaranteed.	3	2	6
121	Project Planning	Given that external commitments were not reviewed with senior management than there is a concern that possibly decisions made by senior management will be counterproductive.	3	2	6
122	Project Planning	Given that a WBS was not developed for the project then there is a concern that possibly, the scope of the project cannot be properly estimated.	5	1	5
123	Project Planning	Given that the project life cycle phases were not defined than there is a concern that possibly the projected schedule will not be adequate for the tasks needed to implement the requirements for this release.	5	1	5
124	Project Planning	Given that major milestones were not identified than there is a concern that possibly the completion of deliverables are not guaranteed.	5	1	5
125	Project Planning	Given that the project plan was not documented than, there is a concern that the project's objectives will not be satisfied.	5	1	5
126	Project Planning	Given that a list of all relevant stakeholders was not included in the project plan than there is a concern that possibly the commitment required to implement the requirements will not be received.	2	2	4

Table 4-10

5.0 COST AND EFFECTIVENESS OF SAFEGUARDS

5.0 COST AND EFFECTIVENESS OF SAFEGUARDS

5.1 Potential Safeguards

Safeguards (mitigation strategies) are a result of the Software Risk Evaluation sessions. The feasibility of each mitigation strategy will be assessed as part of these sessions. To predict feasibility before proper analysis has been done would not serve the project or the customer justice. For a list of potential mitigation strategies, please see Section 4.

5.1.1 Lifecycle Costs for Acceptable Safeguards

Estimation of cost to develop, install, and operate any proposed mitigation strategy will be a result of the Software Risk Evaluation sessions. To predict the cost before proper analysis has been done would not serve the project or the customer justice. For more detail about the Software Risk Evaluation sessions, please see Section 4.

5.1.2 Effect of Safeguards on Risks

Estimating the effectiveness of a mitigation strategy for a particular risk is a result of the Software Risk Evaluation sessions. The effectiveness criterion is established in these sessions and without established criteria, a measurement of effectiveness cannot be conducted with any degree of confidence. To predict effectiveness without quantitative data would not serve the project or the customer justice. For more detail about the Software Risk Evaluation sessions, please see Section 4.

5.1.3 Economic Feasibility of Safeguards

The contrast of the lifecycle costs of each potential mitigation strategy against the financial impact of the risks they are designed to prevent is an analysis that is conducted during the Software Risk Evaluation sessions. The effect each mitigation strategy is projected to have on minimizing those risks is determined based on criteria established in these sessions. Another result of the Software Risk Evaluation sessions is the result of analysis of whether the potential benefits achieved by the mitigation strategies outweigh the project's budgeted costs. For more detail about the Software Risk Evaluation sessions, please see section 4.

6.0 RISK REDUCTION RECOMMENDATIONS

6.0 RISK REDUCTION RECOMMENDATIONS

Risk reduction recommendations will be a result of the Final Report of the Software Risk Evaluation sessions.

7.0 APPENDIX A (LIST OF TABLES)